CYBERSECURITY IN DISTRIBUTION AUTOMATION: APPROACH FOR COMMON REFERENTIAL LEVERAGING STANDARDIZATION

Jean-Luc BATARD
Schneider Electric – France
jean-luc.batard@se.com

Mathieu SALLES
Schneider Electric – France
mathieu.salles@se.com

Eric SUPTITZ
Schneider Electric - France
eric.suptitz@se.com

ABSTRACT

Defining and analyzing a common Cybersecurity requirement referential is today a significant challenge both for Electrical Utilities & Private Customers and for Monitoring & Control Product Suppliers and System Integrators.

This article provides some approach to ease definition and analysis of Cybersecurity requirement during Projects for Distributed Automation Products & Systems, while still taking into account Utility specificities. It is based on appropriate usage of IEC 62443 standard.

HANDLING CYBER REQUIREMENTS DURING REQUEST FOR PROPOSAL: QUITE A CHALLENGE

Request for Proposal process, actors & painpoints

Deploying or extending Distributed Automation Systems by Electrical Utilities or Private Customers (hereafter referred as "Asset Owner") usually involves going through a Request for Proposal process. During this process the Asset Owner expresses his needs. Then Suppliers and System Integrators build and submit their proposal to Asset Owner.

Classical pain points are the difficulty to ensure a common understanding of needs and requirements, and loss of energy by analyzing recurrent requirements instead of focusing on specific aspects.

This paper addresses specifically in this process the pain points related to Cybersecurity requirements encountered by Asset Owners, System Integrator and Product suppliers. Purpose is to propose common language and means leveraging standardization to share expression of needs of the asset owner and enable to focus on project specificities.

Asset Owner specific requirement list

More and more Electrical Utilities and some advanced Private Customers are now aware of Cybersecurity stakes. They engage in securing their Distributed Automation Systems by integrating dedicated requirements related to Cybersecurity in each new Request for Proposal.

However, the way to do it and resulting requirement lists are quite varied:

Current usage for Request for proposal consists most often in extracting from various standards and existing literature (whitepapers, local regulations, …) a list of requirements of different nature related to Cybersecurity.
In best cases, it is based on the output of a risk assessment process.

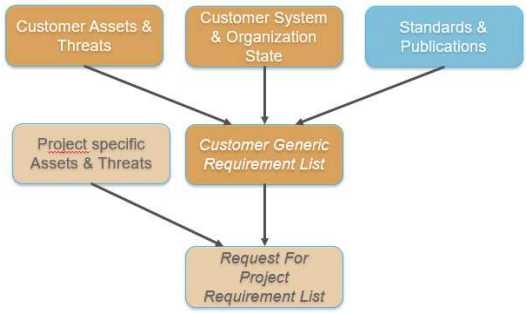

Figure 1: Typical specification process

It may be derived from a generic template or be fully specific to a given tender, then multiplying the number of referential to be maintained by Asset Owner and analyzed by other actors.

Also, maturity level is very diverse: some advanced Asset Owners have themselves contributed strongly to standardization or whitepapers, whereas other are just discovering the jungle of available publications & standards.

As discussed previously in [1], most aspects are in first place related to Asset Owner Organization, Resources and process. Consequently, it is often difficult to clearly separate responsibilities between Asset Owner, System Integrator and Suppliers.

Huge impact for Asset Owners and Suppliers

Consequently, generating the cybersecurity requirement referential requires a strong effort of specification of the Asset Owner, with highly specialized skills.

Care shall be taken to address interoperability issues, length and difficulty of deployment of consistent solution in the field, while keeping door open to competition & multi-sourcing.
Also, this referential must be maintained.
This requires many efforts from Asset Owner specifiers, but also for Suppliers and System Integrators for any new analysis. Getting full traceability of changes like in ADSIC[2] is quite rare, and illustrate perfectly the complexity for all actors…

Next step is a long and fastidious gap analysis for System Integrators and Suppliers for each tender.
It is often followed by a long and costly clarification process with Asset Owner.

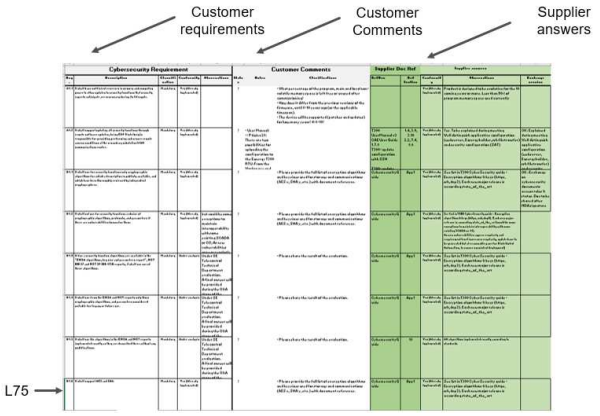

Figure 2: Example of clarification after first gap analysis between Asset Owner and Supplier: many lines, no synthetic view

As the requirement lists are today Asset Owner specific, impact of these complex analysis on Suppliers and System Integrators is expanding drastically.

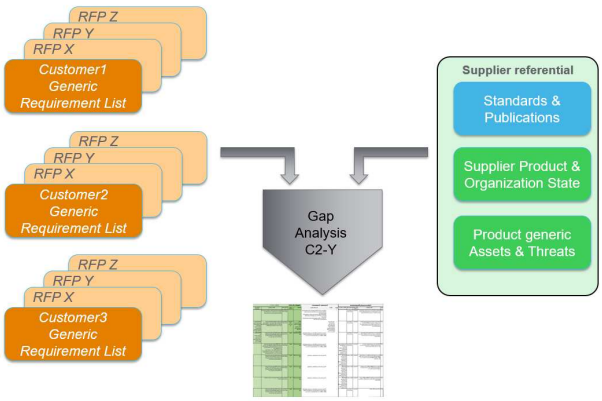

Figure 3: Multiplication of number of referential seen by suppliers

LEVERAGING STANDARDS' FUNCTIONAL REQUIREMENTS

Relying on standardization for Industrial environment

First steps were achieved with ISO/IEC 27000 standard Serie[3], providing a general framework for securing a given organization in IT domain.

Some key whitepapers like ENCS[7] or BDEW[8] go closer to products and systems at OT level and have been typical sources for requirement list until now for advanced Asset Owners.

In addition, key international standards have been developed, addressing actual systems & components and are coming into force.

Various National Regulations have emerged, often reusing most concepts and requirements from standards & whitepapers especially ISO 27000 Serie, but so increasing the number of referential to be analyzed.

As a result, many documents are now available, with various scopes and application domains.

- Some standards provide requirements at functional level.
- Some others at more detailed level are defining technical solutions, like IEC 62351 Serie[6].

It is therefore key in Electrical Distribution domain to select and rely on a well-recognized set of standards.

Managing common reference leveraging International Standard seems to be the obvious way to simplify and define unique language for industrial system among all the different actors: Asset owner, Suppliers and System integrator.

This could help to:

- Share a Common reference for functional capabilities
- Share a Common reference for Certification and Conformance Testing
- Simplify tendering phase and requirements analysis

Approach based on IEC 62443[5]

Specificity of IEC62443 standards series [5] is the covered scope: It addresses the whole product, system and delivery lifecycle, both at features and process level. It does so by addressing perspectives of the different actors. And it is applicable to all industrial automation and control systems (IACS).

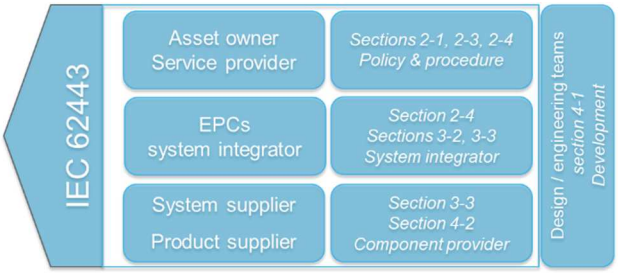

Figure 4: IEC 62443 parts classified per actor

This a specific enrichment for Industrial Control Systems compared to others international standards like ISO/IEC 27000 standard Serie[3].

Important concepts that appear in IEC 62443 standard[5] on the system and product part are:

- Foundational Requirements (FR)
- Security levels (SLs)
- Zones & conduits

Security levels 1 to 4 provide a qualitative approach to addressing security for a zone:

- SL1: Protection against casual or coincidental violation
- SL2: Protection against intentional violation using simple means with low resources, generic skills and low motivation
- SL3: Protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation
- SL4: Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation

The Foundational Requirements are the categories used to organize these technical security controls. Then the Standard defines for each Foundational requirement the detailed control system requirements needed to reach each security level.

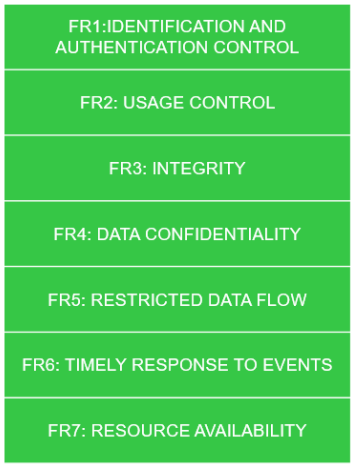

Figure 5: Foundational Requirements

Expected execution in practice expects first asset owner to run a risk analysis by zones & conduits. He then defines counter measures and derives from it the target security levels.
Suppliers and System Integrator have then the capabilities to propose the appropriate security measures, infrastructures and features, for the identified threats and risks.

Link with IEC 62351 Serie[6]

In complement, Asset Owner specification should require that functional system requirements from IEC 62443[5] are implemented in compliance to IEC 62351 Serie[6].

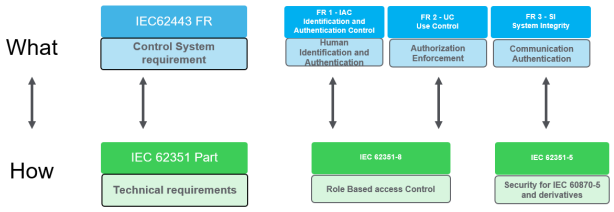

Figure 6: Example of functional system requirement versus technical requirement

For more advanced synthetic view on IEC62443, please refer to [4].

USING FOUNDATIONAL REQUIREMENTS AND SECURITY LEVELS OF IEC 62443 AND ASSOCIATED BENEFITS

Security Level definition per Foundational requirement

By providing a unique well recognized set of security levels based on the list of IEC 62443[5] standard system requirements, specifiers may go quicker and focus on project specificities.

Foundational Requirement	FR1	FR2	FR3	FR4	FR5	FR6	FR7
Required SL	2	2	3	2	1	2	2

Figure 7: High-Level Cybersecurity requirement definition by Asset Owner

Adequate Security Measures following Security Risks analysis

The approach leaves space for the necessary flexibility. By defining different Targeted security levels for the various Foundational Requirement groups, Asset Owner may require more advanced features in some area, while avoiding over-specification in some other depending on Risk analysis.

It allows also for additional requirements hopefully in limited number, to manage pure specificities not addressed by the standard.

One other main interest in the Request for Proposal scope, is to rationalize for Suppliers and System Integrator the functional requirements for Product and System.

Consequently, this will help to Optimize the ratio Effort/Cost/ Risk_coverage to implement "Secure by design" architectures and solutions. For example, it simplifies greatly the clarification process.

Analysis of supplier offers at a glance by Asset Owner and or System Integrator

By comparing required and declared security levels, Asset Owner team will get a straight forward view of the different offers. Decision process is strongly simplified.

Foundational Requirement	FR1	FR2	FR3	FR4	FR5	FR6	FR7
Required SL							
Product1 SL							
Product2 SL							
Product3 SL							

Figure 8: Product analysis for a given RFP by Asset Owner

Clear positioning by Supplier of his offer

By comparing security levels requested by the Asset Owner with already known Security levels of his own solutions, Supplier may select quickly most relevant solutions to propose.

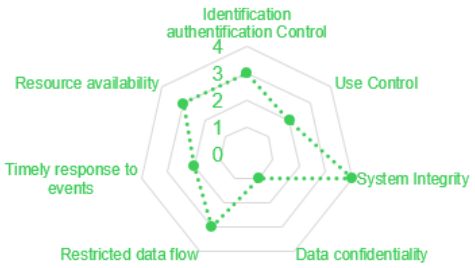

Figure 9: Component Security Levels representation

Going afterwards to an already known list of requirements will enable a quick analysis of compliance of existing offer to Asset Owner Specification.

The same approach coupled with a good knowledge of the market requirements enables to structure a product roadmap at an understandable level. This results in investing efficiently and being able to promote the offer consistently.

Foundational Requirement	FR1	FR2	FR3	FR4	FR5	FR6	FR7
V1	2	2	2	1	2	2	2
V2	4	3	3	2	3	3	2

Figure 10: Component security roadmap high-level definition for supplier

Sound basis towards coming certification

Based on security level profiles defined in IEC 62443[5], it will soon be possible to get components and/or system tested and certified by accredited laboratories.
This will allow confidence that the expected level of security functions is provided by a given component or subsystem.

It will however not yet provide interoperability between Distribution Automation system components if selected technical solutions are not consistent through the whole system.
This will be the goal of future technical profiles based e.g. on IEC 62351 Serie[6]. Hopefully the functional definitions of Security Levels in IEC 62443[5] will be good drivers to build meaningful technical profiles.
Meanwhile asset owners still have to keep explicit requirements on technical solutions.

CONCLUSION

As a conclusion, there is a real opportunity to strongly simplify the specification and tendering process of Cybersecurity aspects for Distributed Automation systems and components, providing very significant benefits to all actors.

This situation is somehow quite comparable as regarding communication protocols in the 80's where private solutions were deployed before going step by step to standards and compliance certification, then to interoperability.

This will require at first a good appropriation of the IEC 62443 standard Serie by all actors, to share a common referential at functional level.

Next steps we may expect are:

- Ensure the official recognition and usage by all actors of IEC 62443 as the reference standard in Request for Proposal.
- Make best usage of allowed flexibility
- Contribute to definition of technical profiles

Hopefully this will be an intermediate step. We should be able to go further towards interworking in the mid- term, by adding 3rd party conformance testing to technical standards. This will become possible once implementation profiles will be defined to select among IEC 62351 technical solutions.

Remembering however that Cybersecurity is a never-ending story, always in movement.

REFERENCES

[1] Jean-Luc Batard, Yves Chollot, Adam Gauci, 2017, "Cybersecurity for modern Distribution Automation Grids", IET Journal, CIRED 2017, 1328

[2] ADSIC, Version 1(2009) and Version 2(2013), "Abu Dhabi Information Security Standards"

[3] ISO/IEC 27001, 2013, “Information technology - Security Techniques - Information security management systems — Requirements”.

[4] Jean-Pierre Hauet, 2016, "Processus et normes de cybersécurité dans l’industrie. L’IEC 62443", CAP'TRONIC Strasbourg

[5] ISO/IEC 62443 Serie, "Security for industrial automation and control systems"

[6] ISO/IEC 62351 Serie, "Power systems management and associated information exchange –Data and communications security"

[7] ENCS - European Network for Cyber Security, 2016, " Distribution Automation RTU Security Requirements "

[8] BDEW - Federal Association of Energy and Water Industries,2008, White Paper "Requirements for Secure Control and Telecommunication Systems",

[9] NERC CIP-002 through CIP-009, " Critical Infrastructure Protection"

[10] NIST Cybersecurity Framework v1.1, 2018, "NIST Cybersecurity Framework"

[11] NIST 800-53 Revision 4 “Security and Privacy Controls for Federal Information Systems and Organizations”

[12] NESA UAE Information Assurance Standards